[2345/62]

SIGNAL TRANSMISSION PROCESS

The present invention relates to a method of transmitting signals according to the definition of the species of Patent Claim 1.

In transmission of signal sequences, authentic transmission of the data or signals always plays a major role. For example, one method of achieving this goal is described in ISO/IEC 9797, Information Technology - Security techniques - Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm (JTC1/SC27 1994). Identical secret keys in combination with an encoding algorithm (block cipher, encipherment algorithm) or with a key-dependent single-way function (cryptographic check function) are assigned to the transmitter and the receiver. This can take place, for example, on a card. The transmitter adds a cryptographic check sum (message authentication code) to each signal (datum) depending on the secret key and the cryptographic algorithm (encoding or single-way function). The receiver in turn calculates the check sum and acknowledges the received signals as authentic if the check sum is identical. However, this method has the following disadvantages: to detect a change in sequence of transmitted data, the check sum of a signal is calculated as a function of the check sum of the signals transmitted previously. Even in the case when a check sum is transmitted after each signal, this is still necessary because otherwise a hacker could record pairs of signal check sums and enter them in an altered sequence without being detected. With the known method, this requires the cryptographic algorithm to be executed for each check sum. Since the sequence and selection of signals are not precisely fixed in advance, it is impossible to calculate the required check sums in advance.

This can lead to problems in a time-critical environment. The cryptographic algorithm can be calculated on a chip card, for example. This is advantageous when using a chip card that has already been evaluated, but otherwise an additional software

achieved by a method composed of a preliminary calculation phase and a communication phase in which the signals or data are transmitted together with the check sums. In the preliminary calculation phase, first a pseudo-random sequence Z is generated by cryptographic algorithms, e.g., a block cipher in the output feedback mode, from the time-variant parameter (sequence number, time mark and other initialization data). As an example, m = 16, 32 or 64 is assumed for a security parameter m. Then nonintersecting strings z(i) of m bits each from sequence Z are assigned to signals s[i], i = 1, 2, ..., n of the signal supply. Additional nonintersecting m-bit strings t[i] are selected from the remaining sequence as the coding of numbers 1, 2, ... MAX, where MAX is the maximum number of signals to be transmitted.

If transmitter authentication is necessary in the subsequent communication phase, then first the sequence of one pass authentication is performed according to the publications ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994) and ISO/IEC 9798-4, Information technology - Security techniques - Entity authentication mechanisms - Part 4: Mechanisms using a cryptographic check function (JTC1/SC27 1995). The transmitter transmits the initialization information and the time-variant parameters to the receiver, and it transmits a number of previously unused bits from Z to the receiver as an authentication token. The receiver in turn calculates pseudo-random sequence Z and checks the received authentication token. The signals received by the receiver during the signal transmission are accepted as authentic if the received authentication token matches the token calculated. In addition, modifications of this method are also possible, as described in detail in the following specification.

The present invention will now be described in greater detail on the basis of embodiments illustrated in the drawing, which shows:

Figure 1 a flow chart for the schematic operation sequence in the receiver, and

Figure 2 a flow chart for the schematic operation sequence in a transmitter.

This method includes a preliminary calculation phase and a communication phase in which the signals are transmitted together with the check sums.

Preliminary calculation phase:

Using the cryptographic algorithm (for example, a block cipher in the output feedback mode according to ISO/IEC 10116, Information Processing - Modes of operation for an n-bit block cipher algorithm (JTC1/SC27 1991)), first a pseudo-random sequence Z is generated from a time-variant parameter (sequence number, time mark, according to ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994)) and other initialization data. Let m be a security parameter, such as M [sic] = 16, 32 or 64. Then from the sequence Z, nonintersecting strings z[i] with m bits each are assigned to signals s(i), i = 1, 2, ..., n of the signal supply. From ...

the authentication token received by the transmitter matches the token calculated.

The sequence of transmitted signals is guaranteed by the influence of the values t[i].

One variant of signal authentication proceeds as follows: If it is necessary to select authentication token T(i) of the i-th signal s[k[i-1]] as a function of all previously transmitted signals s[k[1]], ..., s[k[i-1]], then the token

T(i) = f(t[i], F(i)) can be transmitted for authentication of the i-th signal s[k[i]], where

F(1) = s[k[1]] and

F(i) = f(s[k[i]], F(i-1)) for i > 1.

Calculation of authentication token T(i) thus requires calculation of f twice.

One example of using such a method is the authentic establishment of a connection in making a telephone call. When transmitting the dial tones, it is not known whether an additional dial tone will follow. Therefore, it seems necessary to authenticate each dial tone by transmitting a token in the pause following it. With multi-frequency dialing methods, the length of the dial tones is at least 65 ms, and the length of the pause between dial tones is at least 80 ms. For the authentication described here, this short interval of 145 ms for authentication is sufficient with no problem.

First, the sequence of operations or steps by the receiver are described on the basis of a flow chart according to Figure 1.

In the telephone example, the transmitter is the telephone, optionally equipped with a cryptographic module and/or ...

s[max] = bit (smax-1)*m+1 through bit smax*m of random sequence PRS

t[1] = bit smax*m+1 through bit (smax+1)*m of random sequence PRS

...

t[tmax] = bit (smax+tmax-1)*m+1 through bit (smax+tmax)*m of random sequence PRS

The sequence of operations or steps for the transmitter is described below on the basis of Figure 2.

S3: The transmitter waits for a signal w which is to be transmitted authentically; w is interpreted as a natural number between 1, 2, ..., smax in order to keep the mapping w -> s[w] simple.

S4: The transmitter sends the I-th signal w together with authentication token f(s[w], t[i]). In the telephone example, the token is f(s[w], t[i]) = s[w]⊕t[i], the bit-by-bit XOR of s[w] and t[i].

S5: S3 and S4 are iterated either until no more signals are to be transmitted authentically or until the maximum number of signals that can be authenticated with this supply of previously calculated random sequence PRS has been reached.

S6: In the telephone example, the transmitter is now waiting for a connection to be established with the receiver.

E3, E4 and E5: As long as new signals with the respective authentication tokens are received, the receiver checks on whether the authentication tokens calculated by it match the received tokens.

First, the sequence of operations or steps by the receiver are described on the basis of a flow chart according to Figure 1.

In the telephone example, the transmitter is the telephone, optionally equipped with a cryptographic module and/or chip card, and the receiver is the telephone network, such as the closest exchange.

E1 and S1: The time-invariant parameter here is synchronized between the receiver and transmitter. The time-invariant parameter may be a sequence number or a time mark which has been synchronized. This parameter may optionally also be transmitted as plain text or in encoded form from the transmitter to the receiver for synchronization. In the method according to the present invention, it is expedient that the transmitter already knows the time-invariant parameter before a connection is attempted in order to calculate s[], t[] in advance.

E2 and S2: The transmitter and receiver here first calculate a random sequence PRS (pseudo-random sequence) of length m* (smax + tmax) bits, where

m: security parameter, namely in this example m: = 32.

smax: Maximum number of different signals (number of elements of the alphabets/signal supply). In the telephone example, this refers to digits 1 through 9 and special symbols such as # and others.

tmax: Maximum number of signals to be authenticated in one pass. In the telephone example this would be the maximum length of a telephone number, the maximum number of digits and special symbols for establishing a connection.

Then nonintersecting strings of m bits of this random sequence PRS are assigned to m-bit quantities s[1], s[2], ..., s[smax], t[1], t[2], ..., t[tmax], etc.

s[1] = bit 1 through bit m of the PRS

s[2] = bit m+1 through bit 2*m of the PRS

...

s[max] = bit (smax-1)*m+1 through bit smax*m of random sequence PRS

t[1] = bit smax*m+1 through bit (smax+1)*m of random sequence PRS

t[tmax] = bit (smax+tmax-1)*m+1 through bit (smax+tmax)*m of random sequence PRS

The sequence of operations or steps for the transmitter is described below on the basis of Figure 2.

S3: The transmitter waits for signal w which is to be transmitted authentically; w is interpreted as a natural number between 1, 2, ..., smax in order to keep the mapping w -> s[w] simple.

S4: The transmitter sends the I-th signal w together with authentication token f(s[w], t[i]). In the telephone example, the token is f(s[w], t[i]) = s[w]+t[i], the bit-by-bit XOR link of s[w] and t[i].

S5: S3 and S4 are iterated either until no more signals are to be transmitted authentically or until the maximum number of signals that can be authenticated with this supply of previously calculated random sequence PRS has been reached.

S6: In the telephone example, the transmitter is now waiting for a connection to be established with the receiver.

E3, E4 and E5: As long as new signals with the respective authentication tokens are received, the receiver checks on whether the authentication tokens calculated by it match the received tokens.

E6: If all the tokens match, the received signals are accepted as authentic. In the telephone example, the connection is now established.

E7: If authentication is unsuccessful, no connection is established.